#2

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant(s): CHO, Young-Soon; KANG, Myeong-Joon; KIM, Jae-Young; JUNG, Han

Application No.: Group:

Filed: February 8, 2000 Examiner:

For: DIGITAL DATA FILE ENCRYPTION APPARATUS AND METHOD

L E T T E R

Assistant Commissioner for Patents
Box Patent Application
Washington, D.C. 20231

February 8, 2000
0630-0981P

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55(a), the applicant hereby claims the right of priority based on the following application(s):

Country	Application No.	Filed
REPUBLIC OF KOREA	4483/1999	02/09/99
REPUBLIC OF KOREA	4493/1999	02/09/99

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. 1.16 or under 37 C.F.R. 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By: _____
TERRY L. CLARK
Reg. No. 32,644 Reg No. 35,416
P. O. Box 747
Falls Church, Virginia 22040-0747

Attachment
(703) 205-8000
/wjd

Birch, Stewart et al
703-205-8000
Young-Soon Cho et al
630-981P
1 of 2

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 1999년 특허출원 제4483호
Application Number

출 원 년 월 일 : 1999년 2월 9일
Date of Application

출 원 인 : 엘지전자 주식회사
Applicant(s)

1999 년 6 월 21 일

특 허 청
COMMISSIONER

1999/6/22

【서류명】 출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 2
【제출일자】 1999.02.09
【국제특허분류】 G06F 7/00
【발명의 명칭】 디지탈 데이터 파일 암호화 방법
【발명의 영문명칭】 ENCRYPTION METHOD FOR DIGITAL DATA FILE
【출원인】
【명칭】 엘지전자 주식회사
【출원인코드】 1-1998-000275-8
【대리인】
【성명】 박장원
【대리인코드】 9-1998-000202-3
【포괄위임등록번호】 1999-001894-1
【발명자】
【성명의 국문표기】 김제영
【성명의 영문표기】 KIM,Jae Young
【주민등록번호】 680731-1010319
【우편번호】 142-761
【주소】 서울특별시 강북구 번3동 주공아파트 1단지 103동 504호
【국적】 KR
【발명자】
【성명의 국문표기】 정한
【성명의 영문표기】 JUNG,Han
【주민등록번호】 660715-1066912
【우편번호】 135-270
【주소】 서울특별시 강남구 도곡동 현대아파트 2동 1007호
【국적】 KR
【발명자】
【성명의 국문표기】 조영순
【성명의 영문표기】 CHO,Young Soon
【주민등록번호】 730315-2683915

1999/6/22

【우편번호】	459-110
【주소】	경기도 평택시 지산동 미주2차아파트 104동 612호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 박장원 (인)
【수수료】	
【기본출원료】	10 면 29,000 원
【가산출원료】	0 면 0 원
【우선권주장료】	0 건 0 원
【심사청구료】	4 항 237,000 원
【합계】	266,000 원
【첨부서류】	1. 요약서·명세서(도면)-1통

1999/6/22

【요약서】

【요약】

본 발명은 디지탈 데이터 파일 암호화 방법에 관한 것으로, 종래의 기술에 있어서는 파일 스트림의 암호화시 사용한 암호화 키를 암호화된 파일 스트림의 특정 부분에 모아서 위치시킬 경우 암호화 키가 쉽게 노출될 수 있고, 암호화 키를 파일 스트림에 분산하여 위치시킬 경우에도 최종적으로 해독되어 생성되어야 하는 파일의 형태를 알면 쉽게 암호화 키를 추출해낼 수 있는 문제점이 있었다. 따라서, 본 발명은 디지탈 데이터 플레이어 또는 거기에 사용되는 메모리의 고유번호 등의 정보를 입력받아 여기에 기 약정된 제1 내부키를 더 부가하여 키를 변환하는 제1과정과; 상기 과정에 의해 변환된 키를 제2 내부키에 의해 암호화 알고리즘을 적용하여 암호화된 암호키를 생성하는 제2과정과; 상기 제2과정에 의해 생성된 암호화된 암호키를 이용하여 파일을 암호화하는 제3과정으로 이루어져 암호화 키 자체를 암호화 시킴으로서 파일 스트림에서 암호화 키가 추출 되더라도 이를 해독할 수 없도록 하여 파일 스트림을 복원하지 못하도록 하는 효과가 있다.

【대표도】

도 1

1999/6/22

【명세서】

【발명의 명칭】

디지탈 데이터 파일 암호화 방법{ENCRYPTION METHOD FOR DIGITAL DATA FILE}

【도면의 간단한 설명】

도1은 본 발명에 의해 피씨 및 엠피3와 같은 디지탈 데이터 플레이어에서 파일의 암호화 및 복호화 하는 과정을 보인 블록도.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<2> 본 발명은 파일 암호화 방법에 관한 것으로, 특히 엠피3와 같은 디지탈 데이터의 암호화시에 사용되는 암호키 자체를 암호화 시켜 그 암호화된 암호키를 이용하여 파일 스트림을 암호화 하므로써, 파일 전송 도중 암호키가 해킹되어도 파일 스트림을 복원할 수 없도록 하는 디지탈 데이터 파일 암호화 방법에 관한 것이다.

<3> 여러 디지탈 데이터 중 하나로 엠피3를 예로 들어 설명하면, 엠펙-1(MPEG-1)의 오디오 압축 기술중 압축률이 가장 우수한 레이어-3으로 압축된 엠피3 파일은 아날로그의 음악을 디지탈화 하는 과정(양자화)에서 인간이 들을 수 있는 가청 주파수 범위를 넘는 소리나 특정 악기 소리 뒤에 붙어 전문가가 아니면 듣기 어려운 여운을 빼는 방식으로 만들어져 음질이 좋고, CD데이터의 11배 정도의 압축이 가능한 압축률이 우수한 파일 형태이다.

<4> 따라서, 이미 영화 음악이나 가요 등의 각종 오디오 데이터를 인터넷을 통해 다운로드받아 피씨(PC)의 하드디스크에 저장하고 즐길 뿐 아니라 종래의 휴대용 카셋트에 비해 작은 저장수단에 많은 곡의 저장이 가능하여 휴대용 디지탈 데이터 플레이어의 개발 및 그 사용자가 점차 증가하고 있는 상황이다.

<5> 그러나, 엠피3 파일은 그 특성상 다른 오디오 매체에 비해 복제가 용이하고, 또한 복제시 음질의 저하가 전혀 없는 원음 그대로를 유지할 수 있기 때문에 불특정 다수에

의해 생성 및 복제되어 배포되거나, 음반에 비해 아주 적은 비용으로 음성 유 통되어 음반 저작권자에 대한 저작권을 보호할 수 없게 되었다.

<6> 이에 따라 관련 업계에서는 엠피3 파일에 대한 저작권을 보호할 수 있는 방안이 요구되었고, 그 해결책으로 엠피3 파일에 암호를 걸고, 사용자마다 인증된 키를 주어, 곡을 다운로드할 때 그 키에 맞는 암호를 걸어 배포하는 방식으로 엠피3 파일에 대한 저작권을 보호하게 되었다.

<7> 즉, 각 엠피3 파일 공급자가 공급한 인증된 소프트웨어(엠피3 플레이어)에서는 음악 파일을 재생할 수 있지만, 인증받지 못한 플레이어에서는 잡음만 들리도록 하여 사용자 임의로 재생 및 복제가 불가능하도록 한 것이다.

<8> 상기에서 설명한 바와 같이 디지탈 데이터를 암호화 하는 일반적인 방법은 기본적으로 암호화 키를 발생시키고, 이 키를 이용하여 암호화를 하게 되기 때문에 암호화 키가 해킹되지 않도록 관리하는 것이 무엇보다 중요하다.

【발명이 이루고자 하는 기술적 과제】

<9> 그러나, 상기 종래의 기술에 있어서는 파일 스트림의 암호화시 사용한 암호화 키를 암호화된 파일 스트림의 특정 부분에 모아서 위치시킬 경우 암호화 키가 쉽게 노출될 수 있고, 암호화 키를 파일 스트림에 분산하여 위치시킬 경우에도 최종적으로 해독되어 생성되어야 하는 파일의 형태를 알면 쉽게 암호화 키를 추출해낼 수 있는 문제점이 있었다.

<10> 따라서, 본 발명은 상기와 같은 종래의 문제점을 해결하기 위하여 창출한 것으로, 암호화 키 자체를 암호화 시킴으로서 파일 스트림에서 암호화 키를 추출하더라도 이를

해독할 수 없도록 하여 파일 스트림을 복원하지 못하도록 하는 파일 암호화 방법을 제공 하는데 그 목적이 있다.

【발명의 구성 및 작용】

<11> 이와 같은 목적을 달성하기 위한 본 발명은, 디지탈 데이터 플레이어 또는 거기에 사용되는 메모리의 고유번호 등의 정보를 입력받아 여기에 기 약정된 제1 내부키를 더 포함시켜 키를 변환하는 제1과정과; 상기 과정에 의해 변환된 키를 제2 내부키에 의해 암호화 알고리즘을 적용하여 암호화된 암호키를 생성하는 제2과정과; 상기 제2과정에 의해 생성된 암호화된 암호키를 이용하여 파일을 암호화하는 제3과정으로 이루어짐으로써 달성되는 것으로, 본 발명에 따른 실시예를 첨부된 도면을 참조하여 상세히 설명하면 다음과 같다.

<12> 도1은 본 발명에 의해 피씨 및 엠피3와 같은 디지탈 데이터 플레이어에서 파일의 암호화 및 복호화 하는 과정을 보인 블록도로서, 일단 피씨(1)측에서는 파일을 다운로드(download)시킬 휴대용 엠피3 플레이어(2)가 인터페이스부(미도시)를 통해 접속되면 두 장치간에 기 약속된 제어명령에 의해 상기 엠피3 플레이어(2)나 거기에 사용하는 메모리(미도시)의 고유번호(Serial Number 등)에 관한 정보를 요구하여 입력받게 된다.

<13> 이와 같이 다운로드될 장치의 고유번호 정보를 입력받아 사용자 인증번호로 사용하므로써 따로 사용자 인증과정을 거칠 필요가 없어지게 된다.

<14> 다음, 해킹을 방지하기 위해 상기 입력받은 고유번호에 두 장치(피씨(1)측과 엠피3 플레이어(2))간에 기 약속된 제1 내부키를 더 부가하여 고유번호를 암호키로 사용

하기 위한 변환 과정을 거치게 된다.

<15> 이때 사용하는 제1 내부키는 두 장치간의 약속에 따라서 하나를 부가할 수도 있고 해독을 더 어렵게 하기 위하여 그 이상의 내부키를 부가할 수도 있다.

<16> 이와 같이 장치의 고유번호에 새로운 내부키를 부가하여 암호키로 변환하였으면 종래의 경우에는 바로 이 변환된 암호키를 이용하여 파일을 암호화 시키지만 본 발명에서는 상기 변환된 암호키를 두 장치간의 약속에 따라 제2내부키에 의해 암호키 자체를 암호화 하는 과정을 거치게 된다.

<17> 이때 암호키를 암호화하기 위해 사용되는 암호화 알고리즘은 파일을 암호화하는 알고리즘과는 별도로 키를 암호화하는 알고리즘을 적용할 수 있지만, 휴대용 엠피3 플레이어에서 사용하는 낮은 실행능력을 가진 마이크로프로세서(미도시)를 감안하여 파일 암호화 알고리즘을 같이 적용하므로써 알고리즘을 보관하기 위한 프로그램 메모리의 크기를 줄이고 처리 효율성을 높이도록 한다.

<18> 한편, 상기 과정을 거치는 동안에 다운로드 받는 장치의 고유번호는 내부키가 부가되고, 암호화되어져 암호키 자체를 알아볼 수 없게 되어지고 이하는 종래와 마찬가지로 이 암호키를 이용하여 파일을 암호화 하여 휴대용 엠피3 플레이어로 전송하게 된다.

<19> 이에 따라 휴대용 엠피3 플레이어측에서는 피씨측에서의 상기 암호화 과정과 같은 방법으로 장치의 고유번호에 내부키를 부가하고 여기에 암호화 알고리즘을 적용하여 암호화된 암호키를 복원해 내고, 이를 엠피3 파일의 해독 알고리즘에 적용하여 엠피3 파일을 재생하게 되고, 디코더부를 통해 사운드를 출력하게 된다.

【발명의 효과】

【발명의 효과】

<20> 이상에서 설명한 바와 같이 본 발명 디지탈 데이터 파일 암호화 방법은 암호화 키 자체를 암호화 시킴으로서 장치와 장치간의 데이터 전송 도중 파일 스트림에서 암호화 키가 추출 되더라도 이를 해독할 수 없도록 하므로서 파일 스트림을 복원하지 못하도록 하여 해킹을 방지할 수 있는 효과가 있다.

1999/6/22

1999/6/22

【특허청구범위】

【청구항 1】

디지탈 데이터 플레이어 또는 거기에 사용되는 메모리의 고유번호 등의 정보를 입력받아 여기에 기 약정된 제1 내부키를 더 부가하여 키를 변환하는 제1과정과; 상기 과정에 의해 변환된 키를 제2 내부키에 의해 암호화 알고리즘을 적용하여 암호화된 암호키를 생성하는 제2과정과; 상기 제2과정에 의해 생성된 암호화된 암호키를 이용하여 파일을 암호화하는 제3과정으로 이루어진 것을 특징으로 하는 디지탈 데이터 파일 암호화 방법.

【청구항 2】

제1항에 있어서, 상기 고유번호에 부가되는 제1 내부키는 암호키의 해독을 어렵게 하기 위해서 복수개를 더 부가시킬 수 있도록 한 것을 특징으로 하는 디지탈 데이터 파일 암호화 방법.

【청구항 3】

제1항에 있어서, 상기 키를 암호화 하는 알고리즘은 파일 암호화시에 사용하는 동일한 암호 알고리즘에 의해 생성할 수 있게 한 것을 특징으로 하는 디지탈 데이터 파일 암호화 방법.

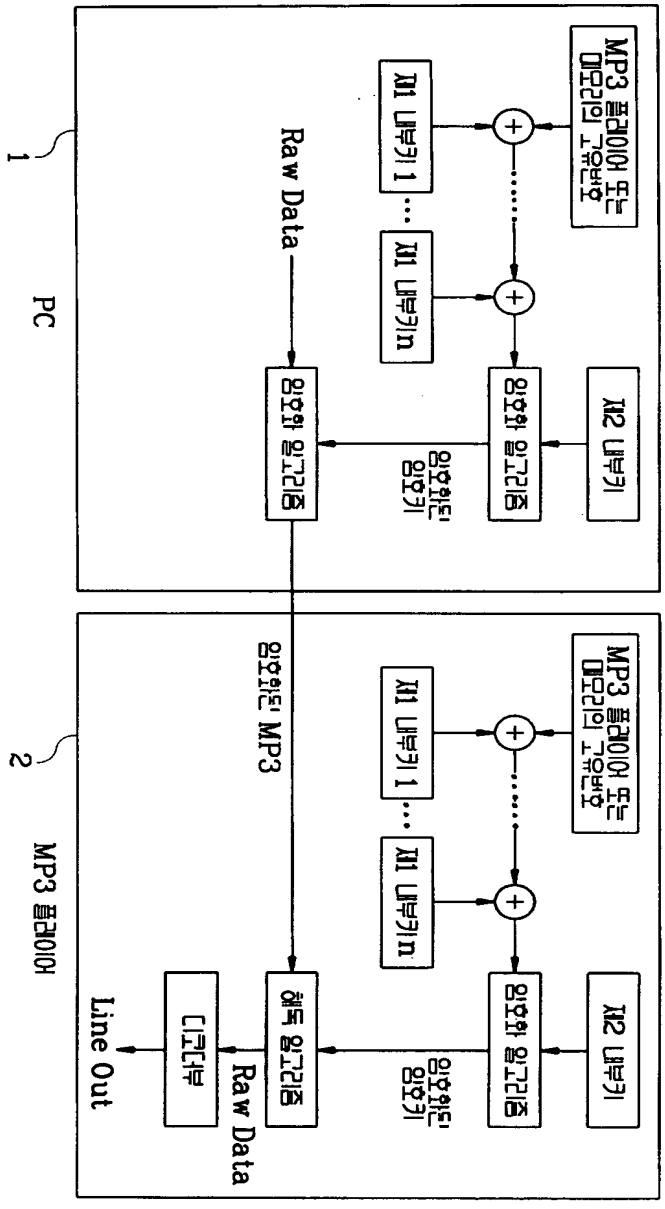
【청구항 4】

제1항에 있어서, 파일을 암호화 하여 전송하는측과 암호화된 파일을 전송받아 해독하는 디지탈 데이터 플레이어측은 암호키를 따로 전송하지 않고 디지탈 데이터 플레이어측의 고유정보를 바탕으로 각각 독립적으로 암호키를 만들기 위한 제1 내부 키

및 제2 내부키를 공유하는 것을 특징으로 하는 디지탈 데이터 파일 암호화 방법.

【도면】

【도 1】


1
PC
MP3 플레이어 또는 메모리의 고유번호
제1 내부키 1
제1 내부키n
제2 내부키
암호화 알고리즘
암호화된 암호키
Raw Data
2
MP3 플레이어
암호화된 MP3
해독 알고리즘
디코더부
Raw Data
Line Out